



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST-NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,108	03/17/2004	Ramarathnam Venkatesan	MS306485.1	5301

27195 7590 12/31/2007  
AMIN. TUROCY & CALVIN, LLP  
24TH FLOOR, NATIONAL CITY CENTER  
1900 EAST NINTH STREET  
CLEVELAND, OH 44114

EXAMINER
----------

SHAN, APRIL YING

ART UNIT	PAPER NUMBER
----------	--------------

2135

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

12/31/2007

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com  
hholmes@thepatentattorneys.com  
osteuball@thepatentattorneys.com

## Office Action Summary

Application No.

10/803,108

Applicant(s)

VENKATESAN ET AL.

Examiner

April Y. Shan

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 15 October 2007 and 21 February 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) 17-33, 35 and 38 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16, 34, 36, 37 and 39 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>6/18/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-16, 34, 36-37 and 39 have been examined.

#### ***Election/Restrictions***

2. Applicant's election Species I (Claims 1-16, 37 and 39), in the reply filed on 15 October 2007 is acknowledged. However, because the Applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (M.P.E.P. § 818.03(a)).

Therefore, Species II (Claims 17-33 and 38) and Species III (Claim 35) ~~are~~ hereby withdrawn from consideration.

#### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 4**, "substantially near..." is being recited. However, it is not clear to the examiner how near of these two elements. Please clarify.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

***Claim Rejections - 35 USC § 101***

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-16, 34, 36-37 and 39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per **claims 1, 34 and 36**, a "system" is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On paragraph [0026] of the original specification, Applicant defines "component" is software and software in execution. As such, it believed that the system of claim 1 is reasonably interpreted as functional descriptive material, per se and as such is not statutory as it fails to fall into a statutory category of invention.

As per **claim 37**, the "computer readable medium" in accordance with Applicant's original disclosure, is signal disclosed in paragraph [0145]. This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Instead, it includes a form of energy. Energy does not fall within a statutory category since it is clearly not a series of steps or acts to constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substances to constitute a composition of matter.

As per **claim 39**, a device employing the system is being recited. However, it appears to the examiner this device is not an element of the claimed system and it is for use with the claimed system. On paragraph [0026] of the original specification, Applicant defines "component" is software and software in execution. As such, it believed that the system of claim 1 is reasonably interpreted as functional descriptive material, per se and as such is not statutory as it fails to fall into a statutory category of invention.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-16, 34, 36-37 and 39 are rejected under 35 U.S.C. 102(b) as being anticipated by Cary ("A MAC Based on Matrix Groups" - published on February 24, 2003).

As per **claims 1, 34 and 37**, Cary discloses a system/data packet (e.g. page 20) that facilitates data transformation, comprising:

a component that receives input data (e.g. pages 15, 16);

and a data transformation component that provides a transformation value for the input data derived from, at least in part, at least one unimodular matrix (e.g. pages 16-18); the transformation value employable to facilitate data protection (e.g. page 7).

As per **claim 2**, Cary further discloses the data transformation component additionally utilizes at least one secret key to provide the transformation value (e.g. pages 14, 16-17).

As per **claim 3**, Cary further discloses the data transformation component utilizes single instruction, multiple data (SIMD) processes to generate the transformation value (e.g. page 14).

As per **claims 4 and 5**, Cary further discloses the data transformation component further provides a d-semi-universal hash, where the d-semi-universal hash possesses a collision probability of two inputs that differ in d locations that is substantially near that of colliding with an independently chosen element of a range (e.g. page 1) and the d-semi-universal hash comprising a 3-semi-universal hash (e.g. pages 16-18).

As per **claim 6**, Cary further discloses the data transformation component further employs at least one inter-block chaining process that utilizes at least one transformation value from a first input data block in determining at least one transformation value for a second input data block (e.g. page 15).

As per **claims 7-8**, Cary further discloses the data transformation component further utilizes at least one transformation value length doubling

process (e.g. pages 16-17) and the transformation value length doubling process comprising a single-pass computational process (e.g. pages 16-17).

As per **claim 9**, Cary further discloses a transformation value encrypting component that encrypts the transformation value provided by the data transformation component (e.g. pages 11-12, 15).

As per **claim 10**, Cary further discloses a streaming cipher component that employs transformation data generated by the data transformation component as at least a portion of a key utilized to encrypt the input data (e.g. page 12).

As per **claim 11**, Cary further discloses the unimodular matrix comprising at least one public matrix (e.g. page 17).

As per **claim 12**, Cary further discloses comprising a reversible system (e.g. page 18).

As per **claims 13 and 14**, Cary further discloses the transformation value comprising a hash value (e.g. page 18) and the hash value comprising a hash value with a collision probability for an input data block of length  $t$  words with  $b$  bit size defined by:  $\Pr[H = H'] = 2^{-4g+20}$ .

where the collision probability is taken over a choice of key,  $H$  and  $H'$  are hash values computed from two distinct inputs, and  $t \leq 50$  (e.g. page 10)

As per **claim 15**, Cary further discloses the data transformation component provides the hash value to at least one selected from the group consisting of a data authentication application and a data integrity application (e.g. pages 6 and 20).

As per **claim 16**, Cary further discloses the data transformation component further provides control of a length of the hash value (e.g. page 14).

As per **claim 37**, Cary discloses the claimed components of the system as applied above in claim 1. Therefore, Cary discloses a computer readable medium having stored thereon the claimed computer executable components of the system.

As per **claim 39**, Cary discloses comprising at least one selected from the group consisting of a computer, a server, and a handheld electronic device (e.g. pages 8 and 20).

### ***Conclusion***

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

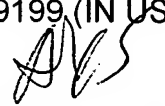


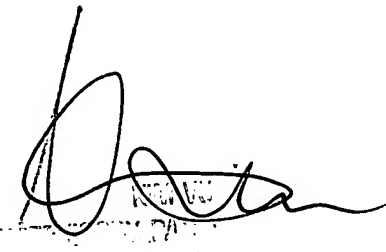
***Contact Information***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
20 December, 2007  
AYS

  
APRIL Y. SHAN  
Examiner